UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,107	02/13/2001	Mihal Lazaridis	555255012189	3129

7590 03/18/2005

David B. Cochran, Esq.
Jones, Day, Reavis & Pogue
North Point, 901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
EDELMAN, BRADLEY E	

ART UNIT	PAPER NUMBER
2153	

DATE MAILED: 03/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/782,107	LAZARIDIS ET AL.	
	Examiner	Art Unit	
	Bradley Edelman	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,44-50,52 and 54-84* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,44-50,52 and 54-84* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/2/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

JE

DETAILED ACTION

This action is in response to Applicant's amendment and request for reconsideration filed on November 26, 2004. Claims 2, 44-50, 52, and 54-84 are presented for examination.

Affidavit Filed Under 37 CFR 1.131

1. Note that the Affidavit filed on August 21, 2003 under 37 CFR 1.131 is NOT sufficient to establish a date of priority of September 29, 1997. Although Examiner previously stated that the Affidavit was sufficient to establish priority, the claims have been amended in such a way that a priority date no longer applies because the material submitted in the affidavit does not support the claim limitation of a "configuration file including encryption information specific to the mobile data communication device." If anything, the submitted affidavit only discloses use of public keys "with a key of 0" (see p. 15 of submitted Document H). In fact, the submitted affidavit clearly teaches that the newly added claim limitation was *not* invented as of the date of the affidavit's submission. In at least three locations, it states that either no encryption, or else only the most simple general encryption is used (see Document D, p. 4, lines 15-16, "there is no compression for cost savings, and no encryption for security being used"; Document E, p. 17, lines 1-3 (also repeated on Document H, p. 19), "Public Key Encryption is the [sic] currently the only foreseen development in stage three. Adding support for Public Key Encryption requires changes to the stack, the messaging sub-system, and possibly the address book as well"; Document E, p. 7, Table, "Encryption:

When working with RIM's Host products all messages will be send [sic] and received using encryption, with a key of 0"). Thus, the affidavit is insufficient to establish a priority date.

Priority

2. Note that although Applicant claimed priority as a continuation to U.S. Patent Application No. 09/087,623, the claims as presently recited were not disclosed in the parent application, and therefore are not afforded priority to that date. Thus, the priority date given to the present application is the *actual* filing date for the present application, which was February 13, 2001.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 2, 44-50, 52, and 54-84 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The independent claims (2, 61, and 70) all discuss a "configuration file including encryption information specific

to the mobile data communication device." This feature was not described in the application as originally filed. The application as originally filed disclosed the following:

a. The *specification* as originally filed only mentioned the word "encrypt" three times:

i. "The repackaging also permits both messages to the mobile device and sent from the mobile device to be encrypted and decrypted as well as compressed and decompressed." Page 7, lines 2-4.

ii. "In preparing the message for redirection, the redirector program 12 could compress the original message A, could compress the message header, or could encrypt the entire message A to created a secure link to the mobile device 24." Page 14, lines 2-4.

iii. "If the system includes encryption keys, these too can be kept at one place for management and update purposes." Page 17, lines 4-5.

Therefore, the specification does not adequately describe the configuration file including encryption information specific to the mobile data communication device, and in fact does not disclose using encryption information specific to the mobile data communication device at all.

b. The *claims* as originally filed in this application (but not in the parent application) disclose the following:

i. Claim 32: "[T]he network host including an encryption key memory store for storing a plurality of unique encryption keys that are used to establish a

plurality of unique secure links between the network host and each of the mobile data communication devices."

ii. Claim 33: "[A]n encryption key database for storing a plurality of encryption keys, wherein each encryption key is associated with a particular user account."

While this adequately describes using unique encryption information for each user account and storing it is a database, it still does not disclose the specific "*configuration file* including encryption information *specific to the mobile data communication device*" as claimed.

For these reasons, the amended claim language constitutes new matter.

The dependent claims are rejected as well for the same reasons as the claims from which they depend.

Examiner suggests that if Applicant desires to include limitations relating to the unique encryption information into the claims, Applicant should use the language as it appeared in the originally filed claims, and should amend the specification to include those features. In such a case, the Application will lose the priority date of May 29, 1998 (parent case) and will also lose any priority claimed in the submitted affidavit.

Claims 57 and 81 are further rejected as constituting new matter. The claim feature that the "redirector component is configured to operate on a server distinct from the messaging server, and is further configured to communicate with the messaging

server using an application programming interface" is not disclosed anywhere in the specification. In contrast, the specification repeatedly states that the redirector program only runs on the host computer (see p. 1, lines 11-12; p. 4, lines 8-9; p. 13, lines 12-20; Figs. 1-3, all showing that the redirector software is only located at the host computer performing the redirection).

Claim 54, 55, 69, and 78-79 are further rejected as constituting new matter. The claim feature of "the redirector component is coupled to the messaging server via a network," or "a network interface for coupling the redirector component to the messaging server" is not described anywhere in the specification. On the contrary, the specification makes it clear that the redirector program only runs on the host computer (see p. 1, lines 11-12; p. 4, lines 8-9; p. 13, lines 12-20; Figs. 1-3, all showing that the redirector software is only located at the host computer performing the redirection), and thus would not communicate with the messaging server via a network interface.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 75 and 76 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "the electronic envelopes" in claims 75 and 76 lack sufficient antecedent basis. It appears that claims 75 and 76 should depend from claim 73, which would provide sufficient antecedent basis.

Note on Claim Language

5. Note, that certain terms used in the claims are broad terms that must be interpreted accordingly. One example of such a term is "coupled," which is used in one instance as follows: "a first network coupled to the redirector component." Such usage of the word "coupled" does not require a direct connection between the network and the redirector component or a particular wire, cable, or other medium between the network and the redirector component. Instead, as defined in Merriam Webster's Collegiate Dictionary, Tenth Edition, the word "coupled" requires only that the two entities are "[brought] into such close proximity as to permit mutual influence" on each other. As another example, the word "in conjunction" merely means "occurring together in time or space," and does not require that the specific time or space be confined to any particularly narrow instance. The claims have been interpreted in view of the broad terminology used therein, as discussed in the claim rejections below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2, 45-47, 52, 56, 58-62, 65-67, 70, 73-75, 77, 80, and 82-84 are rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile Server (AirMobile Wireless Software for Lotus cc:Mail, Communication Server Guide, Motorola, 1995), in view of AirMobile Client (AirMobile Wireless Software for Lotus cc:Mail, Communication Client Guide, Motorola, 1995), and further in view of Gehrmann (PCT Publication No. WO 00/31931).

Note, the AirMobile Server and AirMobile Client guide present different aspects of the same system, and are therefore are treated as a single system for the purposes of this rejection. They are hereinafter referred to together as "AirMobile" with specific citations to the Server guide as "AirMobileS" and the Client guide as "AirMobileC."

In considering claim 1, AirMobile discloses a secure electronic message redirection system (AirMobileS, p. 25, bullet 1, "Motorola AirMobile Wireless for cc:Mail software provides a secure and authenticated virtual wireless communication channel between your laptop and your LAN-based cc:Mail server"), comprising:

A messaging server coupled to a redirector component ("AirMobile Wireless for cc:Mail Server," AirMobileS, P. 10, Fig. 1-1; p. 25, "Overview" ¶ 1, wherein the redirector component is included in the messaging server), wherein the redirector application is configured to sense a trigger event (AirMobileS, "Enable" message, p. 39, Fig. 4-2) and in response to the trigger event to redirect electronic messages received and stored at the messaging server to a mobile data communication device (AirMobileC, p. 17, "Enable/Disable" paragraph; AirMobileS, p. 25, bullet 1, both describing the immediate

forwarding of messages received at the server to the wireless device), wherein the messaging server stores received electronic mail messages in a plurality of mailboxes, each mailbox being associated with a user of a mobile data communication device via a stored configuration file that links the mailbox to a device address of the mobile data communication device (AirMobileS, p. 16);

A first network coupled to the redirector component (Fig. 1-1, the wireline network);

A wireless data network coupled to the mobile data communication device (Fig. 1-1, "wireless data network");

A wireless gateway coupled between the first network and the wireless data network for transmitting messages between the first network and the wireless network (Fig. 1-1, "Wireless network adapter"); and

A secure link formed between the redirector component and mobile data communication device through the wireless gateway, such that messages are secure while being transmitted over the first network, the wireless network, and through the wireless gateway (AirMobileS, p. 25, bullet 1, "secure and authenticated virtual wireless communication channel between your laptop and your LAN-based cc:Mail server").

However, AirMobile remains silent regarding how to implement the security features of the messaging system. Thus, AirMobile does not disclose that the configuration file includes encryption information specific to the mobile data communication device, and that the secure link is formed using an encryption module operating in conjunction with the redirector component that encrypts the electronic

messages prior to redirection to the mobile data communication device using the encryption information stored in the configuration file, and a decryption module operating at the mobile data communication device that decrypts the electronic mail messages received from the redirector component, such that the redirected messages remain encrypted while being transmitted over the first network, the wireless network, and the gateway. Nonetheless, encrypting electronic messages at a server device that works in conjunction with a redirector program for sending electronic messages to a wireless device, wherein the encryption is specific to particular wireless device is well known, as evidenced by Gehrmann (see p. 9, lines 1-18).

In a similar art, Gehrmann discloses a system for forwarding electronic mail messages stored at a server to a user's PDA or other wireless device wherein an encryption unit at the mail server uses "symmetric keys shared between the network mail server 24 and the user's PDA 14" (p. 9, lines 7-8) to encrypt the messages before sending them to the PDA. Thus, given this teaching, it would have been obvious to a person having ordinary skill in the art would have readily recognized the desirability and advantages of creating the secure link taught by AirMobile by using device-specific encryption keys, as taught by Gehrmann, so a user can receive and view secure e-mail via an open network (see Gehrmann, p. 3, lines 27-28), such as the wireless network taught by AirMobile.

Furthermore, although Gehrmann does not disclose storing the keys in a "configuration file," AirMobile discloses storing mobile device specific data in its configuration file (AirMobileS, p. 16), and thus it would have been obvious to use the

same configuration file to store any encryption keys, to avoid the need to build a separate file or database to store user device-specific information.

In considering claim 45, AirMobile further discloses a plurality of personal computers for generating electronic messages, wherein the plurality of personal computers are coupled to the messaging server via a wired network, and wherein the messaging server associates the plurality of mailboxes with the plurality of personal computers (AirMobileS, p. 16, "Adding Additional User Licenses to Your Comm Server"; Fig. 1-1, showing that each user can have an associated cc:Mail client).

In considering claim 46, AirMobile further discloses that the plurality of personal computers are coupled to the messaging server via a LAN (Fig. 1-1, p. 10, describing a LAN).

In considering claim 47, AirMobile discloses generating a trigger event signal using the AirMobile software program (AirMobileC, p. 17). Thus it would have been obvious to generate the event at the user's personal computer, to allow the user to set the parameters for forwarding e-mails from home.

In considering claims 52, 67, and 77, AirMobile further discloses that the redirector component communicates with the messaging server through an API that provides signals to the redirector component when a change occurs to one of the

mailboxes serviced by the messaging server (an API is necessary in AirMobile to allow communications between the redirector component and the server, and would thus provide signals to the redirector component when new messages are received and detected for redirection).

In considering claim 56, AirMobile further discloses that the redirector component is configured to operate on the messaging server (AirMobileS, P. 10, Fig. 1-1; p. 25).

In considering claim 58, AirMobile further discloses that the configuration file is stored at the messaging server (AirMobileS, p. 16).

In considering claim 59, AirMobile further discloses that the configuration file is stored at the server where the redirector component is operating (AirMobileS, p. 16).

In considering claim 60, Gehrmann further discloses that the encryption information includes an encryption key (p. 9, lines 1-18).

Claim 61 describes a redirector component that includes the same features as claimed in claim 2, and is thus rejected for the same reasons.

In considering claim 62, Gehrmann further discloses that the encryption information includes an encryption key for each mobile device (p. 9, lines 1-18).

In considering claim 65, AirMobile further discloses configuring the redirector component to detect a plurality of triggering events that cause the redirection of received and stored messages to the mobile data communication devices, wherein a distinct triggering event can be assigned to each mobile data communication device (AirMobileS, "Enable" message, p. 39, Fig. 4-2; wherein each wireless device can be assigned its own enable trigger).

In considering claim 66, AirMobile further discloses that the triggering events include internal events that occur at the redirector component (AirMobileC, p. 16, "Enable" is set at the server), external events that occur external to the redirector component (AirMobileC, p. 11, wherein filters, which can also serve as triggering events for specific messages, can be changed "from your remote portable"), and network events that are transmitted over a network connection to the redirector component (AirMobileC, p. 11, wherein filters, which can also serve as triggering events for specific messages, can be changed "remotely").

Claim 70 describes a method that includes the same features as claimed in claim 2, and is thus rejected for the same reasons.

Claims 73 and 74 describe the same features as claimed in claim 48, and are thus rejected for the same reasons.

In considering claim 75, as understood, AirMobile further discloses that messages are packaged in electronic envelopes and that the electronic envelopes are e-mail messages addressed to the mobile device and containing the electronic messages (i.e. messages sent via cc:Mail are e-mail messages).

In considering claim 80, AirMobile further discloses that the redirector component is configured to operate on the messaging server (AirMobileS, P. 10, Fig. 1-1; p. 25).

In considering claim 82, AirMobile further discloses that the configuration file is stored at the messaging server (AirMobileS, p. 16).

In considering claim 83, AirMobile further discloses that the configuration file is stored at the server where the redirector component is operating (AirMobileS, p. 16).

In considering claim 84, Gehrmann further discloses that the encryption information includes an encryption key (p. 9, lines 1-18).

7. Claims 44, 48, 49, 63, 64, 71, and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile Server, AirMobile Client, and Gehrmann, and further in view of Nakata et al. (U.S. Patent No. 5,854,841, hereinafter "Nakata").

In considering claims 44, 63, 64, 71, and 72, although the combined teaching of AirMobile and Gehrmann discloses encrypting the electronic messages throughout the transmission process, it does not also disclose compressing the messages. Nonetheless, compressing, in addition to encrypting messages sent across a network, and particularly messages sent from wired to wireless networks, is well known, as evidenced by Nakata. In a similar art, Nakata discloses a system for secure communications between clients and servers across wired and wireless networks, wherein messages sent across the network are both encrypted and compressed to enable secure communication (col. 2, lines 48-57). Nakata even discloses the compressed and encrypted message passes through a gateway device in its transition through the network (col. 14, lines 1-14). Given the teaching of Nakata, a person having ordinary skill in the art would have readily recognized the desirability and advantages of compressing, in addition to encrypting, the messages taught by AirMobile and Gehrmann, in order to conserve bandwidth on the network. Therefore, it would have been obvious to both encrypt and compress the messages in the system taught by AirMobile.

In considering claim 48, the combined teaching of AirMobile, Gehrmann, and Nakata will inherently package the electronic messages into electronic envelopes prior to redirecting them, since they would perform an end-to-end encryption and compression scheme as described above (see specifically, Gehrmann, Abstract, describing the "secure digital envelope").

In considering claim 49, AirMobile further discloses that the electronic envelopes are e-mail messages addressed to the mobile device and containing the electronic messages (i.e. messages sent via cc:Mail are e-mail messages).

8. Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile Server, AirMobile Client, and Gehrmann, further in view of Nakata, and further in view of Picard et al. (U.S. Patent No. 6,233,318, hereinafter "Picard").

In considering claims 50 and 76, although the system taught by AirMobile, Gehrmann and Nakata discloses the use of cc:Mail for sending e-mails from a wired network to a wireless network using IP (Gehrmann, p. 1, lines 20-23), it does not explicitly specify using TCP/IP for communication. Nonetheless, it is well known that cc:Mail can be used across the Internet via TCP/IP, as evidenced by Picard. In a similar art, Picard discloses as system allowing distributed access to electronic messages, and further describes using both TCP/IP and cc:Mail to provide the communication (col. 8, lines 48-54; col. 9, lines 40-49). Thus, TCP/IP is a standard protocol allowing e-mail communications over the Internet, and thus would have been obvious to use with the e-mail system taught by AirMobile in order to facilitate communication over the Internet.

9. Claim 68 is rejected under 35 U.S.C. 103(a) as being unpatentable over AirMobile Server, AirMobile Client, and Gehrmann, in view of Wu et al. (U.S. Patent No. 6,125,369, hereinafter "Wu").

In considering claim 68, although the combined system of AirMobile and Gehrmann inherently uses an API, it does not discuss the specifics of how the API internally works. Nonetheless, Applicant's specification describes using Microsoft's Messaging API (MAPI), a well-known API, and describes that programs such as the well-known MAPI register for notifications or 'advise syncs' when changes to a mailbox take place. This feature is further described by Wu (patent issued to Microsoft), which describes a system for synchronizing data on two devices, and describes the following feature:

> "In still other cases, desktop PIM 16, or a component such as MAPI that is used in conjunction with PIM 16, might be capable of providing an immediate notification to synchronization manager 82 when an object instance is modified in desktop object store 18. For instance, the PIM might allow synchronization manager 82 to register a callback function. In this case, synchronization manager 82 is responsive to these notifications to synchronize the identified objects without polling for changes and without enumerating and comparing handles. When such notifications are provided, changes in desktop object store 18 can be synchronized continuously as they occur, rather than at periodic intervals." (col. 12, line 59 – col. 13, line 3).

Thus, using API notification messages is a well-known way to continuously administer changes in a message store, and it would have been obvious to use the MAPI notifications taught by Wu as the API for detecting new messages in the system taught by AirMobile to avoid the need to build an entirely new, customized API.

Conclusion

Note: This Office action is non-final, due to the new grounds for rejection.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley Edelman whose telephone number is 571-272-3953. The examiner can normally be reached from 9 a.m. to 5 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glen Burgess can be reached at 571-272-3949. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Bradley Edelman

BE
March 16, 2005